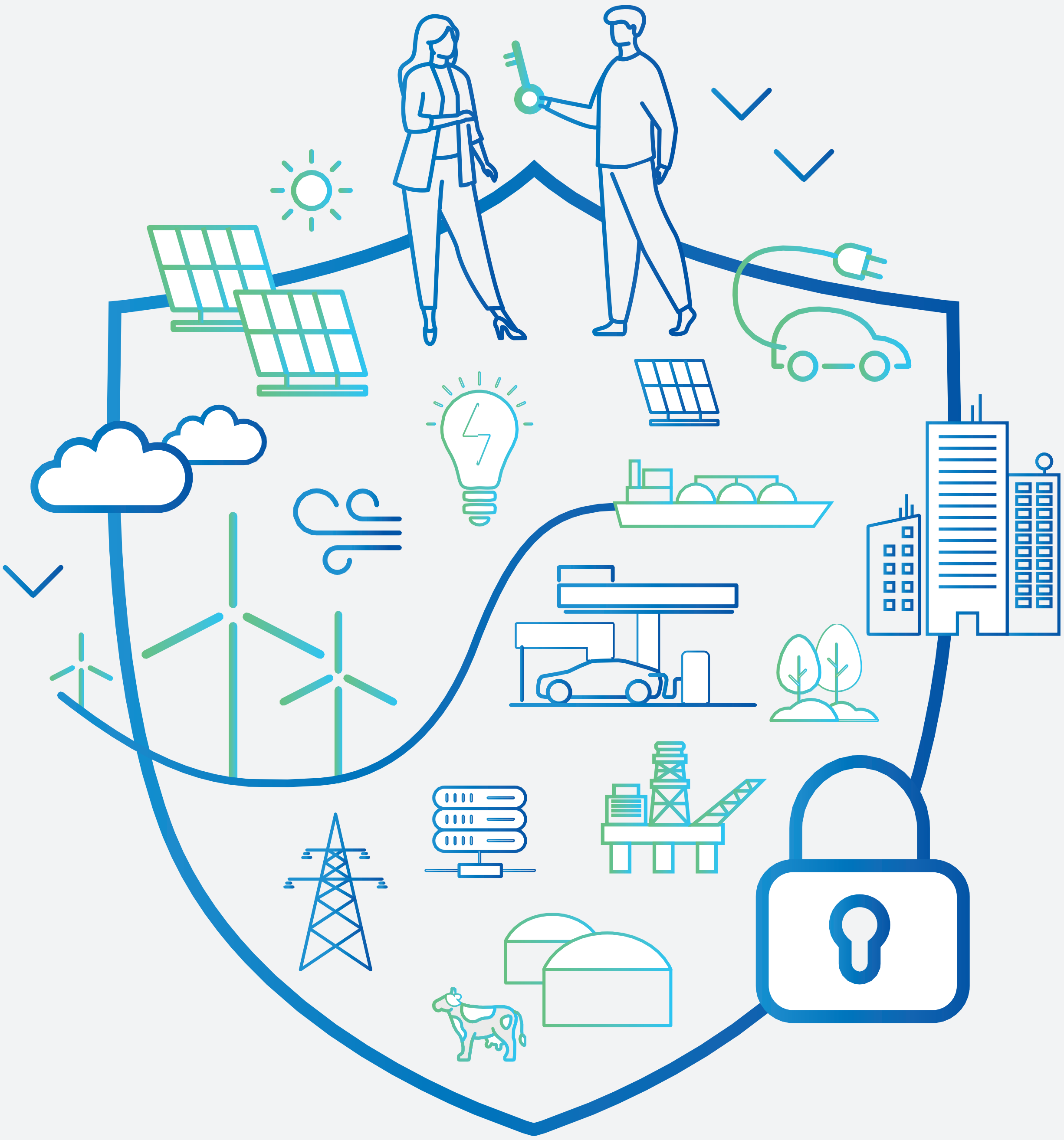


Our **cybersecurity** approach

We have made cybersecurity a priority. A key component of the trust of our customers and our partners, it also contributes to the long-term viability of our activities.

TotalEnergies

DISCLAIMER

The terms «TotalEnergies», «TotalEnergies company» and «Company» in this document are used to refer to TotalEnergies SE and its affiliates included in the scope of consolidation. Similarly, the terms «we», «us», «our» may also be used to refer to these entities or their employees. It cannot be inferred from the use of these expressions that TotalEnergies SE or any of its affiliates is involved in the business or management of any other company of the TotalEnergies company. This publication may contain forward-looking information and statements. They may prove to be inaccurate in the future and are subject to a number of risk factors. Additional information concerning factors, risks and uncertainties that may affect TotalEnergies's financial results or activities is provided in the most recent Registration Document, the French-language version of which is filed with the French securities regulator *Autorité des Marchés Financiers* (AMF), and in Form 20-F filed with the United States Securities and Exchange Commission (SEC).

Brochure published in July 2023.
Thanks to all contributors.

Photo credit
Michel Labelle

Design & production
Inetum

> “The cyber threat will persist and evolve. TotalEnergies has implemented protection, defence and resilience measures in order to keep adapting to the reality of the evolving threat. Thanks to this system, our essential missions can continue to function, regardless of the cyber context.”

Jean-Dominique Nollet
Chief Information Security Officer (CISO)
TotalEnergies

The fundamentals of our cybersecurity approach

- For our entire Company, cybersecurity is a daily priority.
- Our Information Systems (IS) benefit from protection systems that are consistent and tailored to the risk profile.
- Our Company detects attacks, reacts quickly and knows how to rebuild its most critical applications and systems.
- All our IS are integrated within an effective cybersecurity governance, for deploying security measures.

CONTENTS

In this brochure, you can find out about our cybersecurity approach inspired by the NIST Cybersecurity Framework*. It sets out our governance, our organisation, and our activities in the area of protection, maintaining security conditions, detection, reaction and resilience.

The **management of the risks** associated with cybersecurity is a **major issue and priority for our Company.** That's why we deployed a set of **measures** to achieve and maintain **a high level of cybersecurity in line with the threat.**

Our cybersecurity approach is based on **risk management** and **compliance** with the global regulations, and is reflected in:

- **a centralised cybersecurity governance** coordinated by the Chief Information Security Officer (CISO) of our Company;
- **a clear organisation** with a distribution of roles and responsibilities into 3 lines of defence;
- **regular audits and checks** to **test our model.**

Some **core best practices** are also in place to ensure a high level of device, network and data security with:

- the **cybersecurity guidelines**, which have been rolled out to the entire Company, and include the major principles and requirements applicable to people, processes and technologies;
- the Golden Rules for managing the business units and IT;
- a Cyber Pass for regularly **training** our employees in the cybersecurity sector;
- an **awareness-building programme** for all employees.

What's more, our Company wants to ensure that the expectations of our suppliers regarding cybersecurity are sufficient to protect information and our assets, and preserve the continuity of the services they provide to us.

Thanks to technology partnerships with the **Microsoft and Amazon Cloud providers, the security of** our use of their platforms is enhanced.

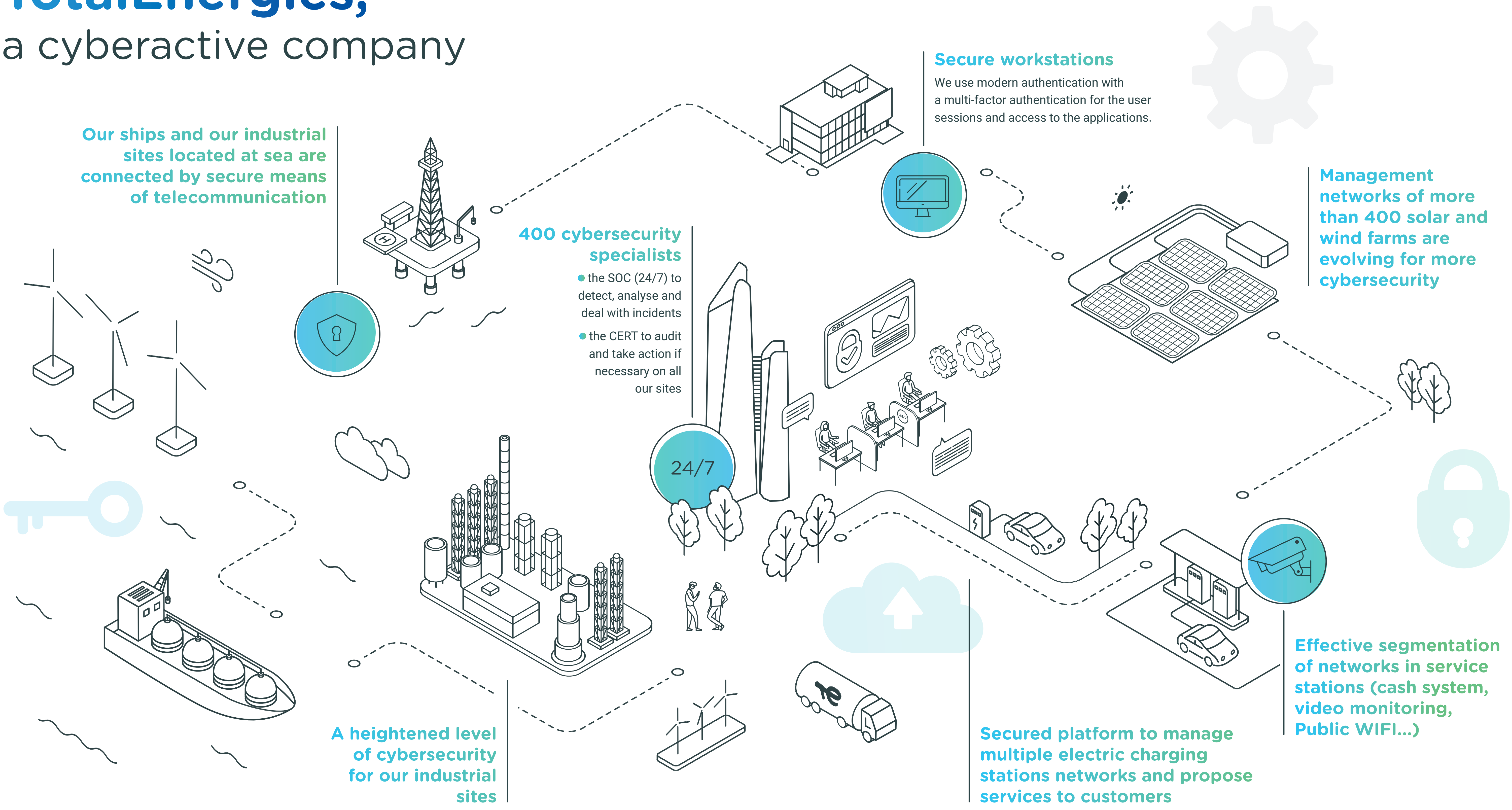
Finally, these protective measures are supplemented by **defence and resilience measures for an appropriate response managed by expert teams** in the event of a cyberattack. In addition, our Company benefits from the following:

- a Security Operations Center **(SOC)** to monitor our Information Systems and detect security incidents;
- a Computer Emergency Response Team **(CERT)**, member of the FIRST**, made up of experts who can react to any cyberattack and have links with other CERTs of large companies in order to share information relating to the threat.

** The cybersecurity framework of the National Institute of Standards and Technology (US federal agency) defines a methodological framework for managing cybersecurity. This framework helps to manage and reduce the cybersecurity risks of Information Systems.*

*** Forum of Incident Response and Security Teams*

TotalEnergies,
a cyberactive company



Our ships and our industrial sites located at sea are connected by secure means of telecommunication

400 cybersecurity specialists

- the SOC (24/7) to detect, analyse and deal with incidents
- the CERT to audit and take action if necessary on all our sites

Secure workstations

We use modern authentication with a multi-factor authentication for the user sessions and access to the applications.

Management networks of more than 400 solar and wind farms are evolving for more cybersecurity

A heightened level of cybersecurity for our industrial sites

Secured platform to manage multiple electric charging stations networks and propose services to customers

Effective segmentation of networks in service stations (cash system, video monitoring, Public WIFI...)

130
countries

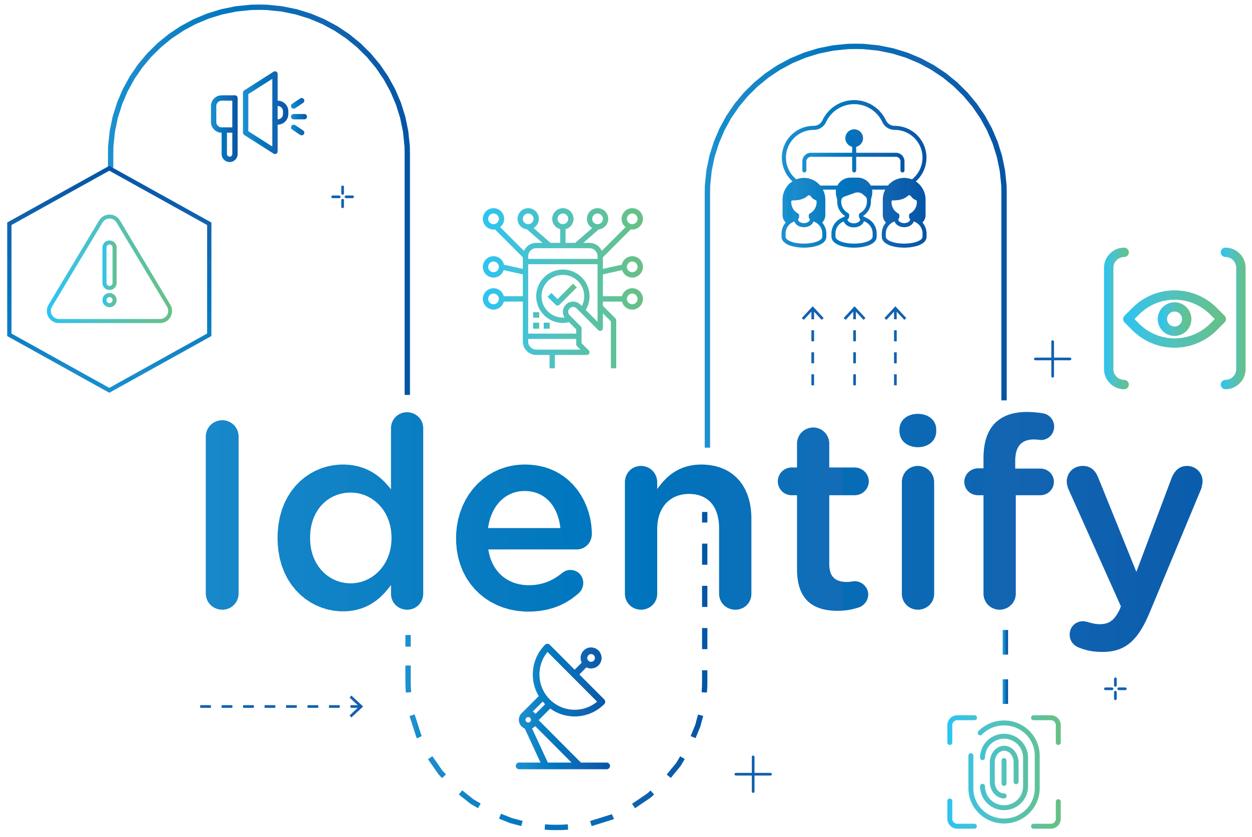
+100,000
workstations

+200,000
public IP addresses

3,900
central applications

14,000
servers

+37,600
terabytes of data



Identify

Cybersecurity governance

Our cybersecurity governance defines the cybersecurity strategy implementation principles of our Company and its affiliates on the one hand, and the roles and responsibilities on the other hand. It relies on managing cybersecurity risks in order to focus on major digital risks and make informed decisions during risk reviews.

It is organised around committees

The **Executive Committee** of our Company validates the cybersecurity strategy and directives.

The **Cybersecurity management committee** is composed of the Chief Information Officer (CIO), the Chief Information Security Officer (CISO) of our Company and the Senior Vice President, Security. The **industrial cybersecurity management committee** also includes the general secretaries of industrial activities, the technical director* and the HSE** director. These two committees make sure that the strategy is properly applied, that any changes to it are defined, and they take the strategic decisions that fall within their respective scope.

The **CISO committee** is made up of all the CISOs of the different activities led by the Company CISO. It translates the strategy into a multi-year cybersecurity programme that sets the cybersecurity priorities of our Company and makes operational decisions.

** HSE: Health Safety Environment   ** In charge of engineering and R&D of our Company's industrial activities*

Common cybersecurity guidelines

Our two cybersecurity directives are shared with all our employees. They are broken down into requirements to be met in order to comply with the level of cybersecurity expected by our Company.

They regulate professional digital uses.

Cybersecurity directive is intended exclusively for IT professionals involved in the construction or running of Information Systems spread throughout the world.

IT usage Directive, aimed at our employees, describes the expected digital uses and behaviours to be avoided.

Scope of the guidelines

The guidelines apply to TotalEnergies SE as well as to any company, in which TotalEnergies SE directly or indirectly holds the majority of the voting rights, and any structure, other than companies, formed in association with third parties and controlled by a company belonging to the Company (including joint ventures, economic interest groups, partnerships, etc.) in accordance with their respective decision-making rules and subject to the legal and regulatory provisions applicable locally.

With regard to companies and structures not controlled by our Company (i.e. which are not controlled by either TotalEnergies SE or by one of its subsidiaries), the representatives of TotalEnergies SE or its subsidiary within these companies or structures, shall endeavour to promote these guidelines in their relations with them.

Content of the guidelines

5	17	172
2 directives 3 rules	guiding principles	requirements

A response that is tailored to each level of risk

The Company's activities are highly dependent on the reliability and security of Information Systems. Each Information System poses a different risk, depending on the threats to which it is exposed, their likelihood and the consequences in the event of a successful cyberattack. The consequences of a cyberattack can be extremely damaging; they can affect the safety of our employees and our facilities, be damaging to our finances, reveal the personal data of our customers or even harm our reputation, and therefore undermine our values and our aims.

A risk-based approach is used to classify the Enterprise and Industrial Information Systems according to a security profile. The implementation of the cybersecurity requirements can be tailored according to this classification. Cybersecurity audits are conducted to ensure compliance with these requirements and assess the likelihood of cyberattacks so that associated action plans can be defined for dealing with the identified risks and controlling them.

3 complementary lines of defence for 3 levels of protection

Line 1 OPERATE

Line 1 is made up our teams who are in charge of a proper operational execution of the cybersecurity measures, preserving the security of the systems and integrating cybersecurity into projects, first and foremost, by analysing the risks.

Line 1 is also involved in **handling the cybersecurity incidents** of their respective remit under the supervision of the SOC or the CERT* depending on the level of gravity.

Line 2 DEFINE and REACT

Line 2 defines the directives and rules compiled in our cybersecurity baseline, and checks that they are properly applied.

It manages business and project related risks, and coordinates cyber crisis management.

It is also responsible for detecting incidents and responding to them.

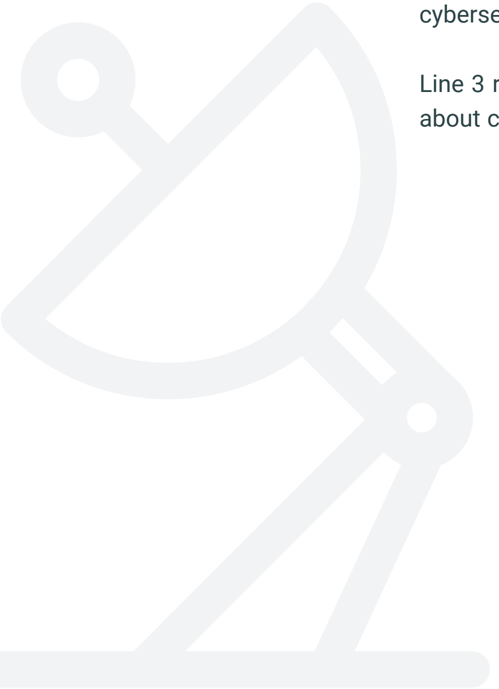
Line 3 CONTROL

Line 3 ensures that the strategy is properly applied and that there are no flaws in the protection, detection and mitigation systems.

Company's Security Division independently assesses the effectiveness of cybersecurity measures put in place. To achieve this, it conducts tests in real-life conditions.

Audit & Internal Control Division conducts compliance audits including cybersecurity governance.

Line 3 reports to Executive committee about critical or major unconformities.



* SOC: Security Operations Center
CERT: Computer Emergency Response Team

Data protection: 3 information protection policies and a dedicated function

We protect our data, that of our customers and partners, and require our suppliers to align themselves with our standards. To do this, we have adopted a consistent approach to protect information at all times.

Within our Company, there are **3 policies** that form the basis for protecting the data held or exchanged. They are used to protect Enterprise and Industrial Information Systems. They apply to all of our activities, head offices and affiliates.

The **personal data protection program** defines the governance and specifies the solutions available within our Company to meet the requirements of the General Data Protection Regulation (GDPR), as well as local regulations.

The **information protection policy** aims to define and enforce the requirements relating to the protection of the confidentiality, integrity and availability of the information held and exchanged within our Company.

Finally, the **document retention policy** aims to define and enforce the requirements regarding document retention.

A dedicated team reporting to the Company CISO is in charge of the information protection process and coordinating the representatives in our Company's business units responsible for implementation and control.

The General Data Protection Regulation (GDPR) came into force on 25 May 2018. The GDPR streamlines the rules in the European Union (EU) by providing a single legal framework to businesses so that they can develop their digital activities based on a relationship of trust with users. However, local laws may stipulate particular or special provisions, which should be taken into account.
The Company has implemented internal corporate rules (Binding Corporate Rules or BCR) approved by the European data protection authorities. They provide a consistent level of protection across our Company when data is transferred by entities located within the EU to Company entities established outside the European Economic Area. These BCR establish the governance of our Company with regard to the protection of personal data by creating a body of internal rules with which each signatory entity is required to comply.

Protective measures tailored to Industrial and Enterprise Information Systems

We separate our Industrial Information System (IIS), which controls our production processes, from our Enterprise Information System (EIS), which is made up of the management processes, servers, and applications that are essential for our employees to run our Company. Specific protection measures apply to each system according to the security requirements.

Separation, differentiate and detect: our 3 key actions to protect our IIS

Our IIS interacts closely with our physical environment through facilities such as motors, valves, sensors and pumps. Given this connection with industrial systems, cybersecurity is of the utmost importance when it comes to the human or environmental consequences, that a malicious act could have on our Industrial Information System.

SEPARATION
in order to prevent propagation

Our first response to protect the IIS and EIS is to keep them physically separate. In this way, in the event of a cyberattack, they can be isolated, which limits the risk of the problem spreading. This separation is achieved by a set of firewalls (bastion) set up within our industrial sites, which restrict and ensure the security of the information exchanged between the two Information Systems. Access for administrators and suppliers passes through bastion (see blue box) hosts that ensure the smooth running of our production activities.

DIFFERENTIATE
in order to provide a tailored solution

In addition to being separated, our IIS is classified into levels according to the criticality of the industrial installations it manages and the associated HSE risks. We use this classification to assign an expected security level or security profile to each Information System. In particular, systems that protect people and industrial installations have the highest level of security, with the strongest protection mechanisms.

INCREASE DETECTION
to secure the industrial process

In order to react as quickly as possible in the event of a cyberattack, we are constantly improving our detection capacity with the support of emerging technologies, in particular. We are working on deploying an Endpoint Detection and Response (EDR) on the industrial scope.

To ensure the protection of our IIS, we have developed our suite of cybersecurity solutions: SAFIIS*. This suite of solutions is deployed on all our critical industrial sites; it is run by a dedicated team and the processing of logs is integrated into our SOC. One of the security services to be implemented is a bastion host that provides secure remote access to our IIS.**

** SAFIIS: Safer Architecture For Industrial Information System*
*** SOC: Security Operations Center*

Renewable energies: new protection *via* the cloud

Our cybersecurity teams support the transformation of our Company towards renewable energies. Our facilities, e.g. wind turbines, solar panels and electric charging stations, cover much larger areas than our oil industry sites. The Information Systems of these activities are largely based on cloud solutions to increase our data processing capacity. We adapted our cybersecurity principles to the cloud platforms by taking advantage of new security technologies. We also modify our approach to the integration of security in Agile Projects and Continuous Integration / Continuous Development process.

The security of the Enterprise Information System: cloud, DevSecOps and XDR suite

AN AMBITIOUS CLOUD STRATEGY
integrating security and compliance

To facilitate our transition to the cloud, we have concluded **two strategic agreements** with the suppliers, **Amazon** and **Microsoft.** These agreements are founded on successful technological partnerships, whose purpose is to add **data redundancy,** make data **permanently availability** and deliver a **high level of security.**

The projects developed in the cloud are in line with our Company's methodology and integrate cybersecurity in each of their phases. Checks are carried out to ensure that our platforms comply with our cybersecurity requirements.

PROCESS
DevSecOps

To integrate data security from start to finish of a project, we have adopted a DevSecOps approach which involves the following:

- an **application code review** focusing on safety and quality with the market-leading solution;
- **a review of the vulnerabilities of the frameworks and the dependence on applications;**
- a **methodology for supporting development projects** by coaches specialised in application cybersecurity.

EXTENDED DETECTION & RESPONSE (XDR) SUITE
to prevent threats and reduce response times

The XDR suite is a set of detection and response solutions installed on our IS (at head offices and in affiliates). These solutions cover all endpoints (desktops, servers and mobiles), messaging, directories and clouds.

This suite provides correlated information to the central cybersecurity teams, giving them access to the most comprehensive view of the vulnerabilities and threats within the scope covered.

The SOC and the CERT* *(see pages 16-17)* therefore have advanced means of investigation, and rapid and effective response capabilities at their disposal to minimise the impact.

Thanks to all of these solutions, we can react quickly to threats, and benefit from regular improvements in protection, detection and response time functions.

The deployment of these solutions gives the SOC a supervision capability on a single console. Thanks to the ease, with which these solutions can be deployed, and their capacity to be extended, any new scope can quickly benefit from operational centralised cybersecurity services.

** SOC: Security Operations Center*
CERT: Computer Emergency Response Team

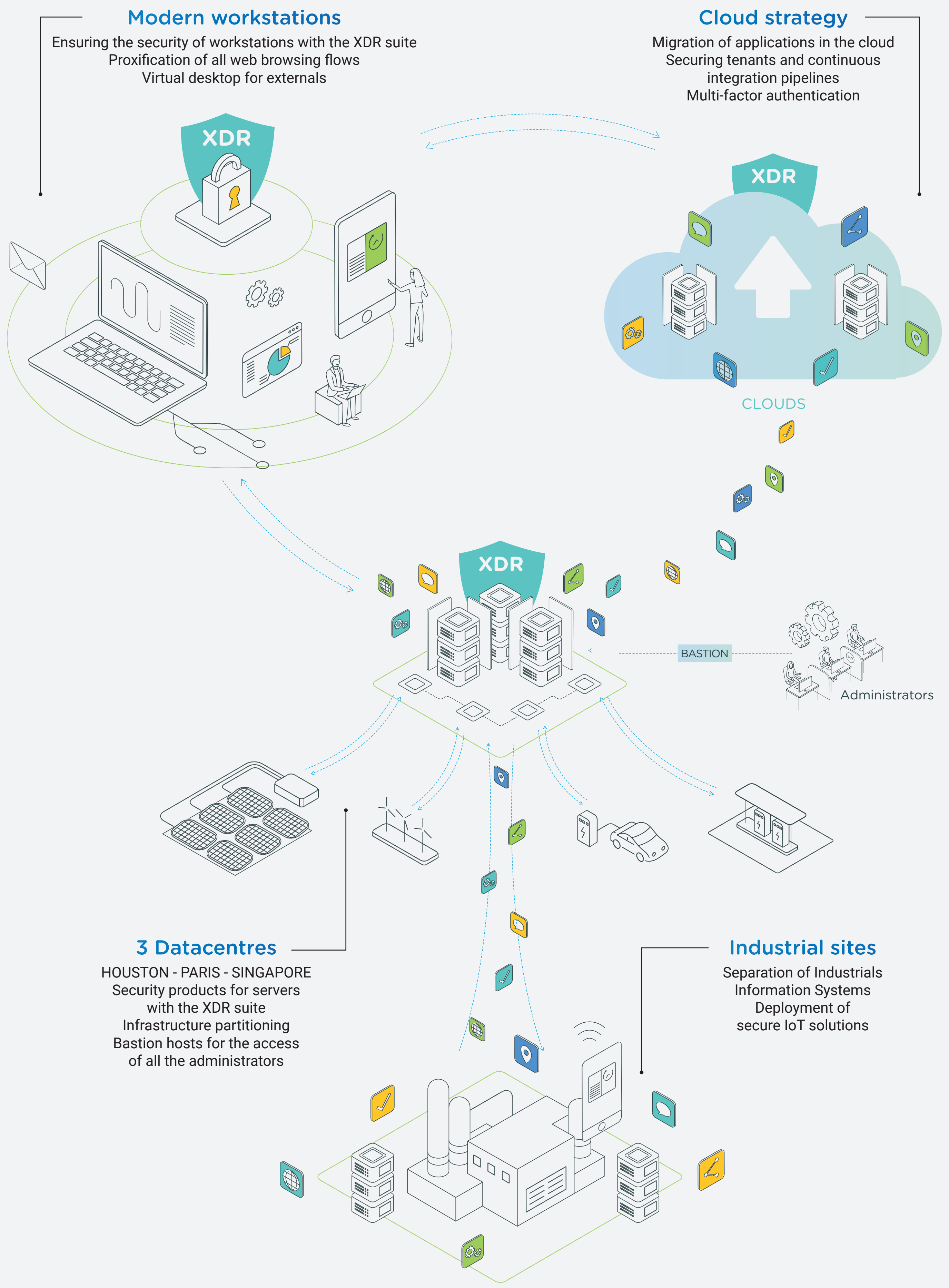
A security assurance plan is mandatory for our suppliers

As for the contracting of services, our partners specify in the security assurance plan the measures and verifications that they will put in place in order to comply with the cybersecurity standards expected by our Company throughout the duration of their service. These commitments are **checked** and **monitored** at scheduled operational and governance committees.

Two contractual clauses are included in the contracts with our suppliers:

- a **cybersecurity clause** defines the expected level of compliance and security: certificates, traceability, external audits, as well as stakeholder training, and confidentiality or responsibility clauses;
- **a clause pertaining to the General Data Protection Regulation (GDPR)** sets out the framework for processing and transferring personal data.

A modern and monitored **ecosystem**



Modern workstations

Ensuring the security of workstations with the XDR suite
Proxification of all web browsing flows
Virtual desktop for externals

Cloud strategy

Migration of applications in the cloud
Securing tenants and continuous integration pipelines
Multi-factor authentication

3 Datacentres

HOUSTON - PARIS - SINGAPORE
Security products for servers with the XDR suite
Infrastructure partitioning
Bastion hosts for the access of all the administrators

Industrial sites

Separation of Industrials Information Systems
Deployment of secure IoT solutions

Awareness-building and training of our employees: cybersecurity is everyone's business

Faced with cyber threats, technical tools and solutions cannot do everything. Our employees, too, have a key role to play. Because they are the first links in our cyber defence chain, we are deploying a training and awareness-building plan to get them involved and help them adopt best practices.

Developing a cyberculture begins with the management

We have defined the Golden Rules, of which three are intended for the business managers and 10 for IT managers. Accountable for compliance with these rules, the managers play an active role in circulating and enforcing these rules within their teams. These are simple but essential requirements, such as "Review data access rights annually and apps" or "Organise an annual cybersecurity crisis drill" on the managed entity. These Golden Rules are deployed within the Company using a "Tone of the top" approach via entity management committees.

Furthermore, in order to build awareness using practical examples, certain incidents are widely circulated to all employees, in the form of an incident sheet as for HSE, starting with the highest level of management.

Dedicated training and Cybersecurity Month

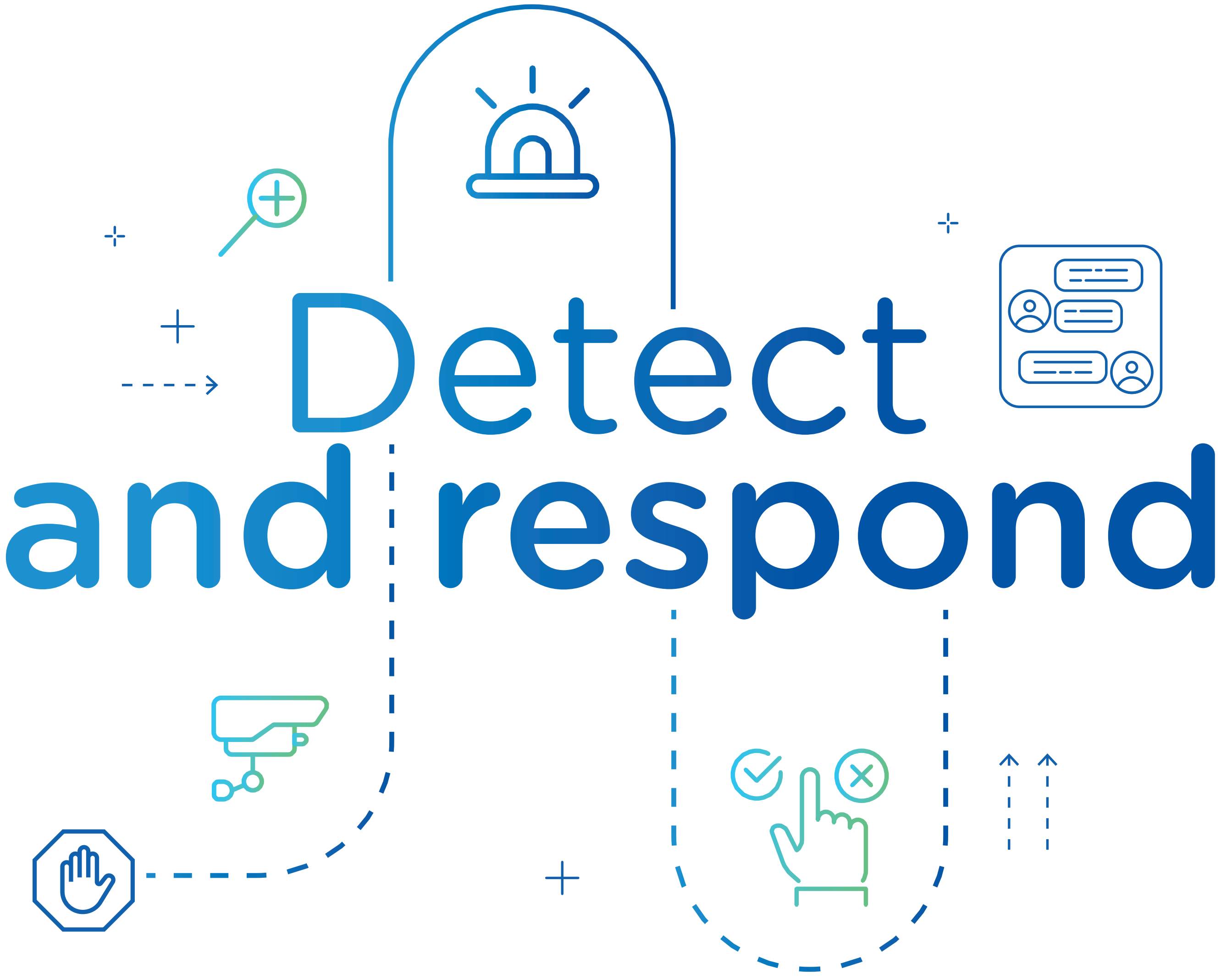
At the same time, we have developed numerous cybersecurity training courses that are available on our e-learning platform. These training courses are also available as classroom lessons conducted on our premises or by carefully selected organisations. Our Company is now developing certified courses based on these training courses that are tailored to the many different profiles of our users, e.g. business manager, IT employee, cybersecurity representative.

Throughout the year, we distribute educational newsletters and carry out awareness-building initiatives. Cybersecurity news and best practices are circulated *via* the intranet and awareness-building messages are issued, e.g. through workstation lock screens. We also carry out phishing campaigns that are global or target a specific site, affiliate or country.

Every year, in October, we hold our Cybersecurity Month during which our 100,000 employees are invited to participate in events and workshops that are specifically tailored to our Company.

With the help of videos, practical case studies and webinars as well as hacking demonstrations on Industrial Information Systems, for example, or live exercises of a phishing attack, they learn to recognise and deal with threats.

The 2022 event was attended by more than 15,000 participants who joined in these activities.



Detect and respond

The Security Operations Center (SOC): a team dedicated to monitoring and analysing cybersecurity events

Every second, and all over the world, the Security Operations Center (SOC) analyses the information from the applications and IS infrastructures used by our businesses. Its role is to detect any unusual signs or behaviour that could indicate a cybersecurity incident. The SOC also works on resolving security incidents and, when these become complex, it works in synergy with the Computer Emergency Response Team (CERT).

The SOC is an internal team made up of enthusiastic cybersecurity experts. This team relies on an outsourced service centre to provide 24/7 supervision. The SOC continuously improves its detection capabilities according to developments in cyber threats and our Company's Information System.

The SOC reminds to employees if necessary the respect of best practices. It learns the lessons from the handling of incidents and puts forward areas for improvement to IS components to prevent these incidents from recurring.

The Computer Emergency Response Team (CERT): a dedicated incident response team

The TotalEnergies CERT is the team in charge of conducting incident response activities and cybersecurity audits within all the entities and affiliates of our Company.

The CERT takes action **on the front line during a cybersecurity crisis:** the team carries out the technical analyses, and decides accordingly and independently on the measures to be taken to resolve an incident, e.g. isolating part of the Information System (IS) to contain a threat, after validation by the Company CISO.
The CERT also takes on **the role of anticipating threats**, not only by **monitoring new vulnerabilities or emerging means of attack** (Threat Intelligence) but also by constantly monitoring the public exposure of our Company.

It conducts dozens of **cybersecurity audits** (organisational test, penetration test, etc.) each year and monitors the resulting action plans. In this way, it makes use of its operational experience in the area of security to contribute to our continuous improvement.

In order to successfully fulfil its duties and be resilient in the event of large-scale attacks, the CERT maintains its own infrastructure, which is totally isolated from the Company's IS. It contains all the applications and tools needed for the smooth running of its activities.

Finally, the CERT **participates in many cooperation groups** on cybersecurity like the FIRST*, InterCERT France** or the Oil and Gas Information Sharing Forum (OGISF).
This cooperation between peers, conducted on a global scale, enhances our intelligence capabilities, gives us access to better information about the new modes of operation of attackers and helps us to identify new threats as soon as possible.

** Forum of Incident Response and Security Teams (cf www.first.org).*
*** InterCERT France is a non-profit (French association law of 1901) and is the first CERT community in France.*

Audits and penetration tests: a stringent programme

We regularly organise audits to draw up an inventory of the security of our Information Systems at a given time in order to highlight potential vulnerabilities and resolve them.

The mode of operation of each test is adapted to the types of assets audited (penetration tests, organisational audit, architecture audit, configuration review).
A report is produced at the end of each audit. The resulting action plan is carefully monitored with requests for documentary evidence. How often the audits are conducted on a particular asset depends, on its level of criticality.

Our responsible disclosure policy: an additional tool for identifying flaws

We have implemented a responsible disclosure policy. It allows anyone who discovers one or more vulnerabilities in our computer systems and networks (websites, mobile apps, etc.) to alert us. It precisely defines and describes the reporting framework and procedures: contact email address, declaration form, respect for the anonymity of the informant, protection of personal data, confidentiality of exchanges, etc.

Recover

Safe remote working

Thanks to the work done to improve the security of the Information System prior to the pandemic and the ongoing work performed during the crisis, the vast majority of our employees were able to continue their remote work activities during the lockdowns, and the cybersecurity teams were able to develop the maturity of our Company's digital security.
By conducting awareness-building campaigns and enhanced training courses dedicated to experts, all the users were also reminded of the need to apply the best practices and behaviours set out in the rule for using Information Systems and resources.

And in the event of a crisis?

Our company has **incorporated cybersecurity into its crisis management system** so that it is prepared and can defend itself against a major crisis caused by a cyberattack. Our cybersecurity crisis management process is structured and organised like that of an industrial or environmental crisis, with the same expectations and resources.

The Crisis Management Cell (CMC) directs the strategic aspects of the crisis situation, e.g. the management of certain stakeholders, communications, the legal and financial aspects, advance preparation for the potential impacts of the current crisis and business continuity. **The Incident Management Team (IMT) leads the tactical response.**

Cyber crisis management exercises, based on specific risk scenarios, are organised each year. They help to get all the stakeholders involved.

Reconstruction of our Information System: full-scale tests to evalue our ability to do a full reset

The only solution to a digital blackout is to prepare to reduce its impact and minimise system downtime. Following this observation, we initiated a multi-year programme of exercises to rebuild our Information Systems.

A LARGE-SCALE TEST

Simulation exercises are conducted under operational conditions and at full-scale. In 2022, 200 people were mobilised for 40 days in 8 countries: IT production teams, external service providers responsible for application maintenance, outsourcing and a certain number of suppliers. The simulation concerned 12 IS perimetres and high-priority business units and 8 applications that support our Company's critical processes as well as the key infrastructure services (Active Directory, orchestrator, hypervisor, etc.): in total, 300 servers, 15 databases and 100 terabytes of backups were tested.

TESTING OUR SYSTEMS TO THEIR LIMITS

Following a full shutdown of our systems, the scenarios plan for a full reset, gradually rebuilding the different layers of the systems, from the lower infrastructure layer to the applications that support our Company's business processes. This unprecedented and innovative approach, in terms of its scope and realism, has many advantages. Firstly, on a human level, it allows us to assess our organisation as well as the resilience of the teams and their ability to carry out coordinated actions in a crisis situation.

Then, from a technical point of view, it gives us the opportunity to test our reconstruction procedures, the security and robustness of our infrastructure, and the performance of our data backup systems to the limit. Finally, we involve our maintenance suppliers and our service providers in these exercises to assess their capabilities and responsiveness. It also gives us an opportunity to compare our operational experience and work methods.

All the information collected during these test phases is compiled, analysed and shared. Following their analysis, new security solutions are identified and optimisation plans are defined that will be deployed and then tested again. Exercises will be conducted on increasingly bigger scopes, in a test-learn-correct-improve virtuous circle that will also reduce stress.

IN FIGURES

200
people mobilised

40
test days

8
maintenance teams involved

> **This exercise, that combines a simulation of a cyberattack, a reconstruction using backups and the mitigation of vulnerabilities, is a first in terms of its scope and realism. It is a pioneering approach for large industrial companies like ours.**

TotalEnergies

TotalEnergies SE

Registered office:
2, place Jean Millier – La Défense 6
92400 Courbevoie – France

Reception:
+33 (0)1 47 44 45 46

Share capital:
€6,225,655,060.00 euros
542 051 180 RCS Nanterre

totalenergies.com